

LISTING OF THE CLAIMS

1. (Previously presented) A system for providing secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components, comprising:
 - a mobile node belonging to a home network located within a secure network; the mobile node having a network interface configured to communicate with other nodes; the mobile node having only one security association and one mobility binding with a Home Agent (HA) for the Mobile IP Home Agent functionality;
 - a Proxy Home Agent (PHA) connected to the home network and located within the secure network, wherein the PHA is configured to provide a proxying functionality;
 - the HA located outside of the secure network, wherein the HA is configured to provide a signaling and tunneling functionality and to notify the PHA of the mobile node; and
 - a VPN gateway located outside the secure network and configured to work in conjunction with the HA.
2. (Original) The system of Claim 1, wherein the VPN gateway and the HA are located within a single device within a DMZ.
3. (Original) The system of Claim 1, further comprising a firewall coupled to the secure network and the VPN gateway; wherein the HA is located within the firewall.
4. (Original) The system of Claim 1, wherein the HA is a separate device from the VPN gateway.
5. (Original) The system according to claim 1, further comprising:
 - a DMZ located outside the secure network, wherein the VPN gateway and the HA reside in the DMZ; a first firewall between the secure network and the DMZ; a second firewall between the DMZ and an external network configured to deny communications from the external

{S:\08212\0200293-US0\80058255.DOC {UNCLASSIFIED//FOR OFFICIAL USE ONLY} }

6. (Original) The system according to claim 1, further comprising:

7. (Previously presented) The system of Claim 1, further comprising a DMZ

8. (Previously presented) The system of Claim 7, wherein packets from the mobile node

9. (Original) The system of Claim 8, wherein packets from the second router to the

11. (Original) The system of Claim 10, wherein the firewall is configured such that it

[illegible]

interface are dropped, and packets with a source address that are within the known address range that are received by the firewall on an external interface are dropped.

12. (Original) The system of Claim 11, wherein VPN encapsulated packets are forwarded to the VPN gateway and when a Security Association (SA) exists, the packet is decrypted and forwarded to the firewall on the internal interface and when a SA does not exist the packet is dropped.

13. (Original) The system of Claim 12, wherein Mobile IP packets and VPN encapsulated packets first reach the Home Agent which are forwarded to the VPN gateway and then to the secure network through the firewall's internal interface.

14. (Previously presented) The system of Claim 1, further comprising a firewall coupled to the secure network and the VPN gateway; and a router includes an access control list used to drop packets that have a source address that belong to a known address range.

15. (Previously presented) A method for secure communication between a mobile node associated with a home network in a secure network and a correspondent node; comprising:

establishing a Proxy Home Agent (PHA) located within the secure network to monitor data directed to the mobile node;

establishing a Home Agent configured to create a security association with the mobile node and to notify the PHA of the mobile node;

collecting data directed to the mobile node;

packaging the collected data in a VPN secure tunnel to an internal address of the mobile node to create VPN packaged data; and

tunneling the VPN packaged data to a current address of the mobile node.

{S:\08212\0200293-US0\80058255.DOC {XX}}